<table>
<tr><td>1.</td><td>Name of Course</td><td colspan="6">Cryptography and network security</td></tr>
<tr><td>2.</td><td>Course Code</td><td colspan="6">CNET4523</td></tr>
<tr><td>3.</td><td>Name(s) of academic staff</td><td colspan="6"></td></tr>
<tr><td>4.</td><td>Rationale for the inclusion of the course/module in the programme</td><td colspan="6">Major
The Great use of local networks and public networks particularly the Internet has raised concerns over security since large volumes of personal, sensitive data and information are now frequently transferred. This module is intended to provide the student With a good understanding of range of network security issues and the methods available to reduce their effects. This module is essential in the preparation of students for future professional career or further study.</td></tr>
<tr><td>5.</td><td>Semester and Year offered</td><td colspan="6">1/4</td></tr>
<tr><td rowspan="3">6.</td><td>Total Student Learning Time (SLT)</td><td colspan="4">Face to Face</td><td colspan="2">Total Guided and Independent Learning</td></tr>
<tr><td rowspan="2">L = Lecture
T = Tutorial
P = Practical
O= Others</td><td>L</td><td>T</td><td>P</td><td>O</td><td rowspan="2">Independent = 84
Total =126</td></tr>
<tr><td>28</td><td>14</td><td></td><td></td></tr>
<tr><td>7.</td><td>Credit Value</td><td colspan="6">3</td></tr>
<tr><td>8.</td><td>Prerequisite (if any)</td><td colspan="6">Computer network CNET3513</td></tr>
<tr><td>9.</td><td colspan="7">Objectives:
To provide solid foundation of the principal of Cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithm.
To provide an awareness of network security issues involving stand alone computers, locally networked computers and remotely networked computers;
To encourage investigation into what factors are likely to result in successful network security
To provide foundations of the basic system security testing for vulnerabilities and procedures of backup and recovery;</td></tr>
<tr><td>10.</td><td colspan="7">Learning outcomes:
On successful completion of the module, students will be able to:
Identify common network security vulnerabilities/attacks
explain the foundations of Cryptography and network security
Critically evaluate the risks and threats to networked computers.
Demonstrate detailed knowledge of the role of encryption to protect data.
Analyze security issues arising from the use of certain types of technologies.
Identify the appropriate procedures required to secure networks.
Identify the appropriate procedures required for system security testing and procedures of Backup and recovery.</td></tr>
<tr><td>11.</td><td colspan="7">Transferable Skills:
Demonstrate detailed knowledge of the role of encryption to protect data.
Exercise judgments on the selection of security processes.
Demonstrate a good knowledge of the procedures used to secure networks.
Professionally communicate about Cryptography and network security with others.</td></tr>
</table>

12. **Teaching-learning and assessment strategy**

A variety of teaching and learning strategies are used throughout the course, including:

- Classroom lessons. Lectures and Power Point presentations
- Tutorial sessions: Practice exercises
- brainstorming;
- student-Lecturer discussion
- collaborative and co-operative learning;
- Independent study.

Assessment strategies include the following:

- Ongoing quizzes
- Midterm tests
- Performance Assessment (project, Assigned exercises)
- Lecturer Observation

13. **Synopsis:**

This module provides ranges of network security issues and the methods available to reduce their effects. It will explore many aspects of network security, including Common network security vulnerabilities/attacks, Types of Cryptographic Functions, Authentication Systems, security standards, firewalls and Network management security.

14. **Mode of Delivery:**

Classroom lessons and Tutorial sessions

15. **Assessment Methods and Types:**

The assessment for this course will be based on the following:

Coursework **50%**

- Quizzes 10%
- Assignments 20%
- Mid-Semester Exam 20%

Final Examination **50%**

100%

16 **Mapping of the course/module to the Programme Aims**

A1	A2	A3	A4	A5	A6	A7	A8	A9
4	4	4	1	5	1	1	2	0

17. **Mapping of the course/module to the Programme Learning Outcomes**

LO1	LO2	LO3	LO4	LO5	LO6	LO7	LO8	LO9	LO10	LO11	LO12
4	3	2	1	2	5	1	2	2	1	0	0

18. **Content outline of the course/module and the SLT per topic**

	Details	SLT			
		L	T	Indep.	Total
Topic 1	**INTRODUCTION** • The History of Information Security, Classical encryption techniques , Internet Crime and computer security threats, Identify attacks as opposed to valid traffic, Common network security vulnerabilities/attacks, Viruses, Worms, Trojan Horses.. Threats from portable code (Plug-ins, Active X, Visual Basic, Java, JavaScript, Flash, Shockwave), Legal Issues. The Multi-level Model of Security,	2	1	6	**9**

	Topic 2	**CRYPTOGRAPHY** Introduction to Cryptography, Types of Cryptographic Functions. **Secret Key Cryptography** • Generic Block Encryption. Data Encryption Standard (DES). International Data Encryption Algorithm (IDEA). Advanced Encryption Standard (AES). **Modes of Operation.** • Encrypting a Large Message. Generating MACs. Multiple Encryption DES. CBC Outside vs. Inside. **Hashes and Message Digests.** • Introduction. Nifty Things to Do with a Hash. MD2. MD4. MD5. SHA-1. HMAC. **Public Key Algorithms**. • Introduction. Modular Arithmetic. RSA. Diffie-Hellman. Digital Signature Standard (DSS). How Secure Are RSA and Diffie-Hellman? Elliptic Curve Cryptography (ECC). Zero Knowledge Proof Systems. **Number Theory.** • Introduction. Modular Arithmetic. Primes. Euclid's Algorithm. Chinese Remainder Theorem. Zn. Euler's Totient Function. Euler's Theorem.	6	3	18	**27**
	Topic 3	**AUTHENTICATION** • Overview of Authentication Systems. Password-Based Authentication. Address-Based Authentication. Cryptographic Authentication Protocols. Who Is Being Authenticated? Passwords as Cryptographic Keys. Eavesdropping and Server Database Reading. Trusted Intermediaries. Session Key Establishment. Delegation **Security Handshake Pitfalls.** • Login Only. Mutual Authentication. Integrity/Encryption for Data. Mediated Authentication (with KDC). Nonce Types. **Strong Password Protocols.** • Introduction. Lamport's Hash. Strong Password Protocols. Strong Password Credentials. Strong Password Credentials Download Protocols	4	2	12	**18**

	Topic 4	**STANDARDS** **Kerberos V4.** Tickets and Ticket-Granting Tickets. Configuration. Logging Into the Network. Replicated KDC's. Realms. Interrealm Authentication. Key Version Numbers. **Kerberos V5.** ASN.1. Names. Delegation of Rights. Ticket Lifetimes. Key Versions.. Cryptographic Algorithms. Hierarchy of Realms. Evading Password-Guessing Attacks. Double TGT Authentication. Kerberos V5 Messages. **PKI (Public Key Infrastructure).** Terminology. PKI Trust Models. Revocation. Directories and PKI. PKIX and X.509. X.509 and PKIX Certificates. Authorization Futures. **Real-time Communication Security.** Session Key Establishment. Perfect Forward Secrecy. PFS-Foilage. Denial-of-Service/Clogging Protection. Endpoint Identifier Hiding. Live Partner Reassurance. Session Resumption. Plausible Deniability **IPsec: AH and ESP.** Overview of Ipsec. IP and Ipv6. AH (Authentication Header). ESP (Encapsulating Security Payload). Comparison of Encodings. **IPsec: IKE.** Photuris. SKIP. History of IKE. IKE Phases. Phase 1 IKE. Phase - 2 IKE: Setting up Ipsec Sas. ISAKMP/IKE Encoding. **SSL/TLS.** Introduction. Using TCP, SSL/TLS Basic Protocol. Session Resumption. Client Authentication. PKI as Deployed by SSL. Version Numbers. Negotiating Cipher Suites. Negotiating Compression Method. Attacks Fixed in v3. Exportability. Encoding.	6	3	18	**27**
	Topic 5	**Electronic Mail Security** Distribution Lists. Store and Forward. Security Services for Electronic Mail. Establishing Keys. Privacy. Authentication of the Source. Message Integrity. Non-Repudiation. Message Flow Confidentiality. Anonymity. Containment. Annoying Text Format Issues. Names and Addresses. • PEM & S/MIME. • PGP (Pretty Good Privacy).	4	2	12	**18**
	Topic 6	**FIREWALLS** Packet Filters. Application Level Gateway. Encrypted Tunnels. Comparisons. Why Firewalls Don't Work. Denial-of-Service Attacks. **Other Security Systems** NetWare V3. NetWare V4. KryptoKnight. DASS/SPX. Lotus Notes Security. DCE Security. Microsoft Windows Security. Network Denial of Service. Clipper.	4	2	12	**18**
	Topic 7	**Network management security** Basic Concepts of SNMP, SNMPv1 Community Facility, SNMPv3. **Testing for system security vulnerabilities;** **Backup and recovery procedures;** **The OSI Security Architecture**	2	1	6	**9**
		Total hours	**28**	**14**	**84**	**126**

19.	**Main references supporting the course:** • William Stallings, **Cryptography and Network Security**: International Edition, Prentice Hall, 2008. • William Stallings**, Network Security Essentials: Applications and Standards:** International Edition, Prentice Hall, 2008.
	Additional references supporting the course: • Charlie Kaufman, Radia Perlman, Mike Speciner, **Network Security: Private Communication in a Public World**, Prentice Hall, 2002
20.	**Other additional information** All materials will be available to the students online.